

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平11-109859

(43)公開日 平成11年(1999)4月23日

(51)Int.Cl.⁶

G 0 9 C 1/00

識別記号

6 5 0

F I

G 0 9 C 1/00

6 5 0 B

6 5 0 Z

G 0 6 F 7/58

G 0 6 F 7/58

A

審査請求 有 請求項の数10 F D (全 10 頁)

(21)出願番号 特願平9-290350

(22)出願日 平成9年(1997)10月6日

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72)発明者 島田 道雄

東京都港区芝五丁目7番1号 日本電気株式会社内

(74)代理人 弁理士 野田 茂

(54)【発明の名称】 擬似乱数発生方法および装置

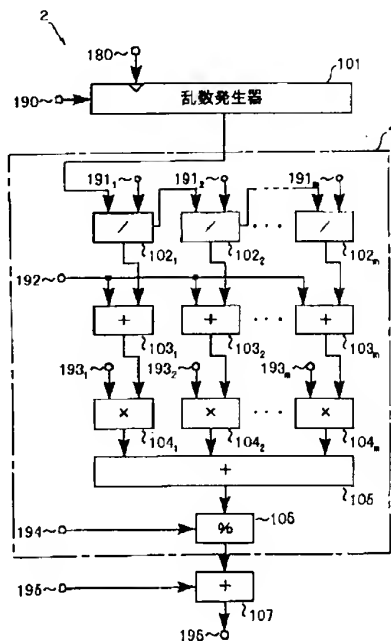
(57)【要約】

【課題】 素数の候補となる整数を短時間で、かつ低コストで生成する。

【解決手段】 乱数発生器101は、入力端子180からのクロックパルスに同期して $0 \leq A < (P_1 - 1)$

$(P_2 - 1) \cdots (P_m - 1)$ を満たす整数Aを無作為に生成する。 P_1, P_2, \cdots, P_m は2以上の素数である。

第1の演算手段4は、この整数Aより、式 $X = a_1 (P_1 P_2 \cdots P_m / P_1) B_1 + a_2 (P_1 P_2 \cdots P_m / P_2) B_2 + \cdots + a_m (P_1 P_2 \cdots P_m / P_m) B_m \pmod{P_1 P_2 \cdots P_m}$ にもとづいて、素数である確率の高い整数Xを算出する。ただし、 a_k ($k = 1, 2, \cdots, m$) は、合同式 $a_k (P_1 P_2 \cdots P_m / P_k) = 1 \pmod{P_k}$ を満たす整数であり、 B_k は $\{A \pmod{(P_k - 1)} + 1$ を表す。加算器107は、整数Xを特定ビット数の整数として出力する。



【特許請求の範囲】

【請求項1】 m を正の整数、 P_1, P_2, \dots, P_m を2以上の素数として、与えられた整数 $(P_1-1)(P_2-1)\dots(P_m-1)$ にもとづき、 $0 \leq A < (P_1-1)(P_2-1)\dots(P_m-1)$ を満たす擬似乱数 A を乱数発生手段により生成する乱数発生ステップと、 D_k を $D_1=A$ で2以上 m 以下の整数 k に対して式 $D_k = D_{k-1} / (P_k - 1)$ により表される複数の整数、 B_k を m 以下の正の整数 k に対して式 $\{D_k \bmod (P_k - 1)\} + 1$ により表される複数の整数、ならびに a_k を合同式 $a_k (P_1 P_2 \dots P_m / P_k) = 1 \pmod{P_k}$ を満たす複数の整数として、式 $a_1 (P_1 P_2 \dots P_m / P_1) B_1 + a_2 (P_1 P_2 \dots P_m / P_2) B_2 + \dots + a_m (P_1 P_2 \dots P_m / P_m) B_m \pmod{P_1 P_2 \dots P_m}$ により表される整数 X を除算手段、剰余演算手段、加算手段、ならびに乗算手段を用いて算出する第1の演算ステップと、 n を正の整数、 Q を条件 $2^{n-1} \leq Q P_1 P_2 \dots P_m$ および $(Q+1) P_1 P_2 \dots P_m \leq 2^n$ を満たす整数として、加算手段により前記整数 X に整数 $Q P_1 P_2 \dots P_m$ を加算して整数を生成し、出力する第2の演算ステップと、を含むことを特徴とする擬似乱数発生方法。

【請求項2】 前記第1の演算ステップは、 $D_1=A$ とし2以上 m 以下の整数 k に対して整数 D_k を整数 (P_k-1) によって除したときの商 $D_{k+1} = D_k / (P_k - 1)$ と剰余 $D_k \bmod (P_k - 1)$ を除算手段により算出する除算ステップと、前記除算ステップで算出した剰余のそれぞれに、第1の加算手段により1を加えて前記複数の整数 B_k をそれぞれ算出する第1の加算ステップと、前記第1の加算ステップで算出した前記複数の整数 B_k のそれぞれに、前記乗算手段を用いて対応する整数 $a_k (P_1 P_2 \dots P_m / P_k)$ を乗じる乗算ステップと、この乗算ステップにおける乗算結果を第2の加算手段によりすべて加算する第2の加算ステップと、この第2の加算ステップにおける加算結果を整数 $P_1 P_2 \dots P_m$ により除したときの剰余を剰余演算手段により算出して前記整数 X とする剰余演算ステップと、を含むことを特徴とする請求項1記載の擬似乱数発生方法。

【請求項3】 m を正の整数、 k を m 以下の正の整数、 P_1, P_2, \dots, P_m を2以上の素数として、与えられた複数の整数 $(P_1-1), (P_2-1), \dots, (P_m-1)$ にもとづき、 $0 \leq A_k < (P_k-1)$ を満たす複数の擬似乱数 A_k を、複数の乱数発生手段によりそれぞれ生成する乱数発生ステップと、 B_k を式 $A_k + 1$ により表される複数の整数、ならびに a_k を合同式 $a_k (P_1 P_2 \dots P_m / P_k) = 1 \pmod{P_k}$ を満たす複数の整数として、式 $a_1 (P_1 P_2 \dots P_m / P_1) B_1 + a_2 (P_1 P_2 \dots P_m / P_2) B_2 + \dots + a_m (P_1 P_2 \dots P_m / P_m) B_m \pmod{P_1 P_2 \dots P_m}$ により表される整数 X を剰余演算手段、加算手段、ならびに乗算手段を用いて算出する第1の演算ステップと、 n を正の整数、 Q を条件 $2^{n-1} \leq Q P_1 P_2 \dots P_m$ および $(Q+1) P_1 P_2 \dots P_m \leq 2^n$ を満たす整数として、前記整数 X に整数 $Q P_1 P_2 \dots P_m$ を加算して整数を生成し、出力する第2の演算手段と、を含むことを特徴とする請求項3記載の擬似乱数発生方法。

$m / P_1) B_1 + a_2 (P_1 P_2 \dots P_m / P_2) B_2 + \dots + a_m (P_1 P_2 \dots P_m / P_m) B_m \pmod{P_1 P_2 \dots P_m}$ により表される整数 X を剰余演算手段、加算手段、ならびに乗算手段を用いて算出する第1の演算ステップと、

n を正の整数、 Q を条件 $2^{n-1} \leq Q P_1 P_2 \dots P_m$ および $(Q+1) P_1 P_2 \dots P_m \leq 2^n$ を満たす整数として、加算手段により前記整数 X に整数 $Q P_1 P_2 \dots P_m$ を加算して整数を生成し、出力する第2の演算ステップと、を含むことを特徴とする擬似乱数発生方法。

【請求項4】 前記第1の演算ステップは、前記乱数発生ステップで生成した前記複数の擬似乱数 A_k のそれぞれに、第1の加算手段により1を加えて前記複数の整数 B_k をそれぞれ算出する第1の加算ステップと、前記第1の加算ステップで算出した前記複数の整数 B_k のそれぞれに、前記乗算手段を用いて対応する整数 $a_k (P_1 P_2 \dots P_m / P_k)$ を乗じる乗算ステップと、この乗算ステップにおける乗算結果を第2の加算手段によりすべて加算する第2の加算ステップと、この第2の加算ステップにおける加算結果を整数 $P_1 P_2 \dots P_m$ により除したときの剰余を剰余演算手段により算出して前記整数 X とする第2の剰余演算ステップと、を含むことを特徴とする請求項3記載の擬似乱数発生方法。

【請求項5】 m を正の整数、 P_1, P_2, \dots, P_m を2以上の素数として、入力された整数 $(P_1-1)(P_2-1)\dots(P_m-1)$ にもとづいて、 $0 \leq A < (P_1-1)(P_2-1)\dots(P_m-1)$ を満たす擬似乱数 A を生成する乱数発生手段と、 D_k を $D_1=A$ で2以上 m 以下の整数 k に対して式 $D_k = D_{k-1} / (P_k - 1)$ により表される複数の整数、 B_k を m 以下の正の整数 k に対して式 $\{D_k \bmod (P_k - 1)\} + 1$ により表される複数の整数、ならびに a_k を合同式 $a_k (P_1 P_2 \dots P_m / P_k) = 1 \pmod{P_k}$ を満たす複数の整数として、式 $a_1 (P_1 P_2 \dots P_m / P_1) B_1 + a_2 (P_1 P_2 \dots P_m / P_2) B_2 + \dots + a_m (P_1 P_2 \dots P_m / P_m) B_m \pmod{P_1 P_2 \dots P_m}$ により表される整数 X を算出する、除算手段、剰余演算手段、加算手段、ならびに乗算手段を含む第1の演算手段と、

n を正の整数、 Q を条件 $2^{n-1} \leq Q P_1 P_2 \dots P_m$ および $(Q+1) P_1 P_2 \dots P_m \leq 2^n$ を満たす整数として、前記整数 X に整数 $Q P_1 P_2 \dots P_m$ を加算して整数を生成し、出力する第2の演算手段と、を含むことを特徴とする擬似乱数発生装置。

【請求項6】 前記第1の演算手段は、前記擬似乱数 A に対して $D_1=A$ とし、2以上 m 以下の整数 k に対して整数 D_k を整数 (P_k-1) によって除したときの商 $D_{k+1} = D_k / (P_k - 1)$ と剰余 $D_k \bmod (P_k - 1)$ を除算手段により算出する複数の除算手段

と、
前記第 1 の剰余演算手段で算出した剰余のそれぞれに 1 を加えて前記複数の整数 B_k をそれぞれ算出する複数の第 1 の加算手段と、
前記第 1 の加算手段で算出した前記複数の整数 B_k のそれぞれに、対応する整数 a_k ($P_1 P_2 \cdots P_m / P_k$) を乗じる複数の前記乗算手段と、
この乗算手段による乗算結果をすべて加算する第 2 の加算手段と、
この第 2 の加算手段による加算結果を整数 $P_1 P_2 \cdots P_m$ により除したときの剰余を算出し、前記整数 X として出力する剰余演算手段と、
を含むことを特徴とする請求項 5 記載の擬似乱数発生装置。

【請求項 7】 m を正の整数、 k を m 以下の正の整数、 P_1, P_2, \dots, P_m を 2 以上の素数として、入力された複数の整数 $(P_1 - 1), (P_2 - 1), \dots, (P_m - 1)$ にもとづいて $0 \leq A_k < (P_k - 1)$ を満たす複数の擬似乱数 A_k をそれぞれ生成する複数の乱数発生手段と、
 B_k を式 $A_k + 1$ により表される複数の整数、ならびに a_k を合同式 $a_k (P_1 P_2 \cdots P_m / P_k) = 1 \pmod{P_k}$ を満たす複数の整数として、式 $a_1 (P_1 P_2 \cdots P_m / P_1) B_1 + a_2 (P_1 P_2 \cdots P_m / P_2) B_2 + \cdots + a_m (P_1 P_2 \cdots P_m / P_m) B_m \pmod{P_1 P_2 \cdots P_m}$ により表される整数 X を算出する、剰余演算手段、加算手段、ならびに乗算手段を含む第 1 の演算手段と、
 n を正の整数、 Q を条件 $2^{n-1} \leq Q P_1 P_2 \cdots P_m$ および $(Q + 1) P_1 P_2 \cdots P_m \leq 2^n$ を満たす整数として、前記整数 X に整数 $Q P_1 P_2 \cdots P_m$ を加算して整数を生成し、出力する第 2 の演算手段と、
を含むことを特徴とする擬似乱数発生装置。

【請求項 8】 前記第 1 の演算手段は、
前記乱数発生手段で生成した前記複数の擬似乱数 A_k のそれぞれに 1 を加えて前記複数の整数 B_k をそれぞれ算出する複数の第 1 の加算手段と、
前記第 1 の加算手段で算出した前記複数の整数 B_k のそれぞれに、対応する整数 a_k ($P_1 P_2 \cdots P_m / P_k$) を乗じる複数の前記乗算手段と、
この乗算手段における乗算結果をすべて加算する第 2 の加算手段と、
この第 2 の加算手段における加算結果を整数 $P_1 P_2 \cdots P_m$ により除したときの剰余を算出し、前記整数 X として出力する剰余演算手段と、
を含むことを特徴とする請求項 7 記載の擬似乱数発生装置。

【請求項 9】 前記乗算手段は ROM により構成されていることを特徴とする請求項 6 または 8 に記載の擬似乱数発生装置。

【請求項 10】 前記の剰余演算手段は、
第 1 および第 2 の ROM と第 1 および第 2 の加算器とを含み、
前記第 2 の加算手段の出力データを構成する複数のビットのうち、下位側の複数のビットは前記第 1 の加算器の一方の入力端子に供給され、残りのビットは前記第 1 の ROM のアドレス端子に供給され、前記第 1 の ROM の出力データは前記第 1 の加算器のもう一方入力端子に供給されており、
前記第 1 の加算器の出力データを構成する前記複数のビットのうち、下位側の複数のビットは前記第 2 の加算器の一方の入力端子に供給され、残りのビットは前記第 2 の ROM のアドレス端子に供給され、前記第 2 の ROM の出力データは前記第 2 の加算器のもう一方入力端子に供給されており、
前記第 2 の加算器の出力データが前記の剰余演算手段の前記剰余の算出結果として出力されることを特徴とする請求項 6 または 8 に記載の擬似乱数発生装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は擬似乱数を発生する方法および装置に関するものである。

【0002】

【従来の技術】従来より、電話、モデム、あるいはテレビジョンなどの通信システムにおける伝送情報が第三者によって盗聴されないようにするため、送信情報に擬似乱数を排他的論理和加算することで送信情報の暗号化が行われている。暗号化の方式には暗号化と復号化とで同一の鍵を用いる慣用暗号と、暗号化と復号化とで異なる鍵を用いる公開鍵暗号の 2 つの技術が知られている。このうち公開鍵暗号方式は、鍵を通信に先だって予め配送しておく必要がないので手間が省け、また鍵の管理は受信側でのみ行えばよいので鍵の管理が容易であるという利点を有する。

【0003】公開鍵暗号方式では、受信側は秘密鍵を用いて情報の復号化を行い、この秘密鍵には通常数百ビットから数千ビットもの桁を有する素数が用いられる。したがってこのようなビット数の多い素数を無作為にいかん効率よく生成するかが重要な課題となっている。

【0004】このような素数の生成には公式が存在しないので、特定のビット数の素数を生成する場合、基本的には、まず特定ビット数の整数を無作為に生成し、それが素数かどうかを判定するということを、素数が得られるまで繰り返す必要がある。しかし、素数か否かを判定するためには多量の計算が必要なため、従来は、単に特定ビット数の整数を無作為に生成するのではなく、素数の候補として、素数である確率の高い整数をまず生成し、その整数に対して素数か否かの判定を行うことで時間の短縮を図っていた。

【0005】図 4 はこのような従来の素数の候補を生成

する方法を示すフローチャートである。この図に示すように、まず、 n を正の整数として n ビットの整数 X （擬似乱数）を無作為に生成する（手順410）。ただし、その整数 X が偶数であれば明らかに素数ではなく、また、その整数 X は上位ビットが零のために n ビットでない場合もあるので、その整数 X の最下位ビットと最上位ビットを1にする（手順420）。次に、正の整数 j を1とし（手順430）、 X が P_j で割り切れるかどうかを検査し、 X が P_j で割り切れる場合は手順410に制御を移し、一方、割り切れない場合は、手順450に制御を移す。手順450では、 $j=m$ か否かを検査し、 $j=m$ ならば処理を終了して X を素数の候補（擬似乱数）として出力し、 $j=m$ でなければ手順460に制御を移す。手順460では、 $j=j+1$ とし、制御を440に移す。なお、ここで、 m は予め決められた正の整数であり、 P_1, P_2, \dots, P_m は互いに異なる小さい素数である。こうにして整数 X を生成すれば、 X が、 P_1, P_2, \dots, P_m を素因数に持つことがないので、単純に無作為に生成しただけの n ビットの整数よりも素数である確率が高くなり、効率よく特定ビット数の素数を得ることができる。

【0006】なお、従来の素数生成方法および公開鍵暗号については、例えばシュナイア著「アブライド・クリプトグラフィー（第2版）」（Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition, John Wiley & Sons, Inc. 1996）などに詳しく解説されている。

【0007】

【発明が解決しようとする課題】しかし、無作為に生成された n ビットの整数が素数である確率は、素数定理からすると、約 $1/n$ 程度であることが知られている。したがって、従来の方法では、1つの素数の候補を得るために約 n 個の整数を無作為に生成する必要があった。そして、秘密鍵としては上述のように数百から数千のビット数の素数が用いられるので、このような秘密鍵の候補を1つ得るために、整数を数百回から数千回も生成し、そのたびに生成した整数を素数 P_j で除して整数が P_j で割り切れるか否かを確認しなければならず、多量の演算を行う必要があった。そのため、素数の候補を得るために時間がかかり、また、除算を実行するために除算器が必要であり、装置は高コストとなっていた。

【0008】そこで本発明の目的は、素数の候補となる整数を短時間で、かつ低コストで生成できる擬似乱数発生方法および装置を提供することにある。

【0009】

【課題を解決するための手段】本発明の擬似乱数発生方法は上記目的を達成するため、 m を正の整数、 P_1, P_2, \dots, P_m を2以上の素数として、与えられた整数

$(P_1-1)(P_2-1)\dots(P_m-1)$ にもとづき、 $0 \leq A < (P_1-1)(P_2-1)\dots(P_m-1)$ を満たす擬似乱数 A を乱数発生手段により生成する乱数発生ステップと、 D_k を $D_1=A$ で2以上 m 以下の整数 k に対して式 $D_k = D_{k-1} / (P_k-1)$ により表される複数の整数、 B_k を m 以下の正の整数 k に対して式 $(D_k \bmod (P_k-1)) + 1$ により表される複数の整数、ならびに a_k を合同式 $a_k (P_1 P_2 \dots P_m / P_k) = 1 \pmod{P_k}$ を満たす複数の整数として、式 $a_1 (P_1 P_2 \dots P_m / P_1) B_1 + a_2 (P_1 P_2 \dots P_m / P_2) B_2 + \dots + a_m (P_1 P_2 \dots P_m / P_m) B_m \pmod{P_1 P_2 \dots P_m}$ により表される整数 X を除算手段、剰余演算手段、加算手段、ならびに乗算手段を用いて算出する第1の演算ステップと、 n を正の整数、 Q を条件 $2^{n-1} \leq Q P_1 P_2 \dots P_m$ および $(Q+1) P_1 P_2 \dots P_m \leq 2^n$ を満たす整数として、加算手段により前記整数 X に整数 $Q P_1 P_2 \dots P_m$ を加算して整数を生成し、出力する第2の演算ステップと、を含むことを特徴とする。

【0010】また、本発明の擬似乱数発生方法は、 m を正の整数、 k を m 以下の正の整数、 P_1, P_2, \dots, P_m を2以上の素数として、与えられた複数の整数 $(P_1-1), (P_2-1), \dots, (P_m-1)$ にもとづき、 $0 \leq A_k < (P_k-1)$ を満たす複数の擬似乱数 A_k を、複数の乱数発生手段によりそれぞれ生成する乱数発生ステップと、 B_k を式 $A_k + 1$ により表される複数の整数、ならびに a_k を合同式 $a_k (P_1 P_2 \dots P_m / P_k) = 1 \pmod{P_k}$ を満たす複数の整数として、式 $a_1 (P_1 P_2 \dots P_m / P_1) B_1 + a_2 (P_1 P_2 \dots P_m / P_2) B_2 + \dots + a_m (P_1 P_2 \dots P_m / P_m) B_m \pmod{P_1 P_2 \dots P_m}$ により表される整数 X を剰余演算手段、加算手段、ならびに乗算手段を用いて算出する第1の演算ステップと、 n を正の整数、 Q を条件 $2^{n-1} \leq Q P_1 P_2 \dots P_m$ および $(Q+1) P_1 P_2 \dots P_m \leq 2^n$ を満たす整数として、加算手段により前記整数 X に整数 $Q P_1 P_2 \dots P_m$ を加算して整数を生成し、出力する第2の演算ステップと、を含むことを特徴とする。

【0011】そして、本発明の擬似乱数発生装置は、 m を正の整数、 P_1, P_2, \dots, P_m を2以上の素数として、入力された整数 $(P_1-1)(P_2-1)\dots(P_m-1)$ にもとづいて、 $0 \leq A < (P_1-1)(P_2-1)\dots(P_m-1)$ を満たす擬似乱数 A を生成する乱数発生手段と、 D_k を $D_1=A$ で2以上 m 以下の整数 k に対して式 $D_k = D_{k-1} / (P_k-1)$ により表される複数の整数、 B_k を m 以下の正の整数 k に対して式 $(D_k \bmod (P_k-1)) + 1$ により表される複数の整数、ならびに a_k を合同式 $a_k (P_1 P_2 \dots P_m / P_k) = 1 \pmod{P_k}$ を満たす複数の整数として、式 $a_1 (P_1 P_2 \dots P_m / P_1) B_1 + a_2 (P_1 P_2 \dots P_m / P_2) B_2 + \dots + a_m (P_1 P_2 \dots P_m / P_m) B_m \pmod{P_1 P_2 \dots P_m}$ により表される整数 X を算出する、除

算手段、剰余演算手段、加算手段、ならびに乗算手段を含む第1の演算手段と、 n を正の整数、 Q を条件 $2^{n-1} \leq Q P_1 P_2 \cdots P_m$ および $(Q+1) P_1 P_2 \cdots P_m \leq 2^n$ を満たす整数として、前記整数 X に整数 $Q P_1 P_2 \cdots P_m$ を加算して整数を生成し、出力する第2の演算手段と、を含むことを特徴とする。

【0012】また、本発明の擬似乱数発生装置は、 m を正の整数、 k を m 以下の正の整数、 P_1, P_2, \dots, P_m を2以上の素数として、入力された複数の整数 $(P_1-1), (P_2-1), \dots, (P_m-1)$ にもとづいて $0 \leq A_k < (P_k-1)$ を満たす複数の擬似乱数 A_k をそれぞれ生成する複数の乱数発生手段と、 B_k を式 $A_k + 1$ により表される前記複数の整数、ならびに a_k を合同式 $a_k (P_1 P_2 \cdots P_m / P_k) = 1 \pmod{P_k}$ を満たす複数の整数として、式 $a_1 (P_1 P_2 \cdots P_m / P_1) B_1 + a_2 (P_1 P_2 \cdots P_m / P_2) B_2 + \cdots + a_m (P_1 P_2 \cdots P_m / P_m) B_m \pmod{P_1 P_2 \cdots P_m}$ により表される整数 X を算出する、剰余演算手段、加算手段、ならびに乗算手段を含む第1の演算手段と、 n を正の整数、 Q を条件 $2^{n-1} \leq Q P_1 P_2 \cdots P_m$ および $(Q+1) P_1 P_2 \cdots P_m \leq 2^n$ を満たす整数として、前記整数 X に整数 $Q P_1 P_2 \cdots P_m$ を加算して整数を生成し、出力する第2の演算手段と、を含むことを特徴とする。

【0013】与えられた任意の非負整数 D_k に対して、 $\{D_k \bmod (P_k-1)\} + 1$ で表される上記整数 B_k は、 $0 < B_k < P_k$ を満たす。 $0 < B_k < P_k$ であれば、 $B_k \neq 0 \pmod{P_k}$ である。したがって、 P_1, P_2, \dots, P_m が相異なる素数ならば、連立1次合同式 $X = B_1 \pmod{P_1}, X = B_2 \pmod{P_2}, \dots, X = B_m \pmod{P_m}$ の解が存在し、その解を X (上記整数 X) とすると、 X は P_1, P_2, \dots, P_m のいずれによっても割り切れない。すなわち、 X が m 個の小さな素数 P_1, P_2, \dots, P_m を素因数に持たないということになり、 X が素数である確率は、単に無作為に与えられた整数が素数である確率よりも高くなる。

【0014】そして、上記連立1次合同式の解 X は、 $X = a_1 (P_1 P_2 \cdots P_m / P_1) B_1 + a_2 (P_1 P_2 \cdots P_m / P_2) B_2 + \cdots + a_m (P_1 P_2 \cdots P_m / P_m) B_m \pmod{P_1 P_2 \cdots P_m}$ によって簡単に求められることが知られており、最初に1つの擬似乱数 A を生成する本発明の擬似乱数発生方法および装置では、上記第1の演算ステップおよび第1の演算手段において、この式により整数 X を算出する。また、上記第2の演算ステップおよび第2の演算手段では、整数 X に $Q P_1 P_2 \cdots P_m$ を加算するので、 n ビットの整数が最終出力として得られる。

【0015】最初に複数の擬似乱数 A_k を生成する本発明の擬似乱数発生方法および装置では、乱数発生ステップ

および乱数発生手段で上記 $D_k \bmod (P_k-1)$ に相当する擬似乱数 A_k を生成し、第1の演算ステップおよび第1の演算手段ではこの擬似乱数 A_k により整数 X を算出し、さらに、第2の演算ステップおよび第2の演算手段では上記発明の場合と同様に、 n ビットの整数を生成する。

【0016】

【発明の実施の形態】次に本発明の実施の形態について図面を参照して説明する。図1は本発明による擬似乱数発生装置の一実施の形態を示す機能ブロック図である。以下ではこの図を参照して本発明による擬似乱数発生装置の一実施の形態について説明し、同時に、対応する本発明による擬似乱数発生方法の一実施の形態について説明する。

【0017】この擬似乱数発生装置2は、公開鍵暗号方式の秘密鍵とする素数の候補を生成するためのものであり、図1に示したように、本発明に係わる乱数発生手段としての乱数発生器101、本発明に係わる第1の演算手段4、本発明に係わる第2の演算手段としての加算器107により構成されている。そして、第1の演算手段4は、除算器102₁、102₂、……、102_m (本発明に係わる除算手段)、加算器103₁、103₂、……、103_m (本発明に係わる第1の加算手段)、乗算器104₁、104₂、……、104_m (本発明に係わる乗算手段)、加算器105 (本発明に係わる第2の加算手段)、剰余演算器106 (本発明に係わる剰余演算手段) により構成されている。

【0018】乱数発生器101には、入力端子180を通じてクロック信号が供給され、一方、入力端子190を通じて整数 $(P_1-1), (P_2-1), \dots, (P_m-1)$ が入力されている。ここで、 m は正の整数、 P_1, P_2, \dots, P_m は2以上の素数である。そして、乱数発生器101は、上記クロック信号の各クロックパルスに同期して $0 \leq A < (P_1-1), (P_2-1), \dots, (P_m-1)$ を満たす擬似乱数 A を生成し、第1の演算手段4に出力する。

【0019】第1の演算手段4の機能は、次の【数1】にもとづいて、素数である確率の高い整数 X (擬似乱数) を算出することである。

【0020】

【数1】 $X = a_1 (P_1 P_2 \cdots P_m / P_1) B_1 + a_2 (P_1 P_2 \cdots P_m / P_2) B_2 + \cdots + a_m (P_1 P_2 \cdots P_m / P_m) B_m \pmod{P_1 P_2 \cdots P_m}$
ここで、 a_k ($k=1, 2, \dots, m$) は、合同式 $a_k (P_1 P_2 \cdots P_m / P_k) = 1 \pmod{P_k}$ を満たす整数である。また、 B_1, B_2, \dots, B_k は、式 $B_k = \{D_k \bmod (P_k-1)\} + 1$ によって値の決められる複数の整数であり、ここで、 D_1, D_2, \dots, D_m は、 $D_1 = A$ 、2以上の k に対しては $D_k = D_{k-1} / (P_{k-1}-1)$ によって値の決められる複数の整数である。

なお、[数1]により表される整数 X が、素数である確率が高い整数であることの理由については後に詳しく説明する。

【0021】第1の演算手段4を構成する各除算器102 k ($k=1, 2, \dots, m$) には、端子191 k を通じて整数 (P_k-1) が入力されて、また、除算器1021には、乱数発生器101から上記擬似乱数 A が入力されている。そして、除算器1021は擬似乱数 A を整数 (P_1-1) によって除したときの商 $D_2=A/(P_1-1)$ と剰余 $A \bmod (P_1-1)$ を算出して、商と剰余を出力し、各除算器102 k ($k=2, \dots, m$) は、左側の除算器102 $k-1$ の出力する商 D_k を整数 (P_k-1) によって除したときの商 $D_{k+1}=(D_k/(P_k-1))$ と剰余 $D_k \bmod (P_k-1)$ を算出し、商と剰余を出力する。なお、各除算器102 k ($k=1, 2, \dots, m$) の出力する剰余は、それぞれ対応する各加算器103 k に出力される。なお、以下では説明の便宜上 $D_1=A$ と表記する。各加算器103 k には、各除算器102 k からの上記剰余と共に、入力端子192を通じて“1”が入力されており、各加算器103 k は剰余 $D_k \bmod (P_k-1)$ に1を加え、結果を整数 $B_k=(D_k \bmod (P_k-1)) + 1$ として対応する各乗算器104 k に出力する。

【0022】各乗算器104 k には、各加算器103 k による加算結果 B_k と共に、各端子193 k を通じて整数 $a_k (P_1 P_2 \dots P_m / P_k)$ が入力されており、乗算器104 k は、この整数と上記加算結果 B_k との積を算出し、結果を加算器105に出力する。ここで a_k は、合同式 $a_k (P_1 P_2 \dots P_m / P_k) = 1 \pmod{P_k}$ を満たす整数である。加算器105は、各乗算器104 k の出力をすべて加算し、加算結果を剰余演算器106に出力する。剰余演算器106には、この加算結果と共に、端子194を通じて素数 P_1, P_2, \dots, P_m の積としての整数 $P_1 P_2 \dots P_m$ が入力されており、剰余演算器106は加算器105からの加算結果を整数 $P_1 P_2 \dots P_m$ で除した時の剰余を算出し、整数 X として加算器107に出力する。

【0023】加算器107には、剰余演算器106からの整数 X と共に入力端子195を通じて上記整数 $P_1 P_2 \dots P_m$ に整数 Q を乗じた整数 $Q P_1 P_2 \dots P_m$ が入力されており、加算器107はこれらの整数を加算し、得られた整数(擬似乱数)を、秘密鍵とする素数の候補として出力する。ここで、 Q は、条件 $2^{n-1} \leq Q P_1 P_2 \dots P_m$ および $(Q+1) P_1 P_2 \dots P_m \leq 2^n$ を満たす整数である。

【0024】次に、このように構成された擬似乱数発生装置2の動作について説明する。乱数発生器101は、入力端子180を通じてクロック信号の1つのクロックパルスが入力されると、そのクロックパルスに同期して $0 \leq A < (P_1-1)(P_2-1) \dots (P_m-1)$ を満

たす整数 A (擬似乱数)を無作為に生成し、除算器1021に供給する(本発明に係わる乱数発生ステップ)。

【0025】これに対して、除算器1021は、擬似乱数 A を整数 (P_1-1) によって除したときの商 $D_2=A/(P_1-1)$ と剰余 $A \bmod (P_1-1)$ を算出して、商と剰余を出力し、各除算器102 k ($k=2, \dots, m$) は、左側の除算器102 $k-1$ の出力する商 D_k を整数 (P_k-1) によって除したときの商 $D_{k+1}=D_k/(P_k-1)$ と剰余 $D_k \bmod (P_k-1)$ を算出し、商と剰余を出力し、剰余をそれぞれ対応する加算器103 k に出力する(本発明に係わる除算ステップ)。なお、以下では説明の便宜上 $D_1=A$ と表記する。そして、各加算器103 k は、各剰余演算器102 k からの剰余 $D_k \bmod (P_k-1)$ に、入力端子192を通じて入力されている“1”を加え、結果 $B_k=(D_k \bmod (P_k-1)) + 1$ を対応する乗算器104 k に出力する(本発明に係わる第1の加算ステップ)。乗算器104 k は、この加算結果 B_k に、対応する入力端子193 k を通じて入力されている整数 $a_k (P_1 P_2 \dots P_m / P_k)$ を乗じ、結果を加算器105に出力する(本発明に係わる乗算ステップ)。

【0026】その後、加算器105は、各乗算器104 k の出力をすべて加算して加算結果を剰余演算器106に出力し(本発明に係わる第2の加算ステップ)、剰余演算器106は、加算器105からの加算結果を、入力端子194を通じて入力されている整数 $P_1 P_2 \dots P_m$ で除した時の剰余を算出して加算器107に整数 X として出力する(本発明に係わる剰余演算ステップ)。

【0027】そして、加算器107は、剰余演算器106からの上記整数 X に、入力端子195を通じて入力されている整数 $Q P_1 P_2 \dots P_m$ を加算し、得られた整数(擬似乱数)を、秘密鍵とする素数の候補として出力端子196より出力する(本発明に係わる第2の演算ステップ)。[数1]にもとづいて算出された上記整数 X は、 $0 \leq X < P_1 P_2 \dots P_m$ を満たす整数であるから、所望のビット数、すなわち n ビットの整数であるとは限らない。しかし、加算器107により、条件 $2^{n-1} \leq Q P_1 P_2 \dots P_m$ および $(Q+1) P_1 P_2 \dots P_m \leq 2^n$ を満たす整数 Q を整数 $P_1 P_2 \dots P_m$ に乘じた整数 $Q P_1 P_2 \dots P_m$ を整数 X に加算することで、 n ビットの整数が得られる。その結果、入力端子180を通じて乱数発生器101にクロックパルスが入力されることに、公開鍵暗号方式における秘密鍵とするための n ビットの素数の候補が出力端子196を通じて次々に出力される。なお、上記 m の値は、 Q の値が存在する範囲でできるだけ大きく選ぶことが、素数である確率がより高い擬似乱数を得る上で好ましい。

【0028】ここで上記[数1]がいかに導出されるかについて、また、整数 X が素数の候補となり得る理由について詳しく説明する。与えられた任意の非負整数 D_k

に対して、 $B_k = \{D_k \bmod (P_k - 1)\} + 1$ で表される上記整数 B_k は、 $0 < B_k < P_k$ を満たす。 $0 < B_k < P_k$ であれば、 $B_k \neq 0 \pmod{P_k}$ である。したがって、 P_1, P_2, \dots, P_m が相異なる素数であれば、連立1次合同式 $X = B_1 \pmod{P_1}$ 、 $X = B_2 \pmod{P_2}$ 、 \dots 、 $X = B_m \pmod{P_m}$ の解が存在し、その解を X (上記整数 X) とすると、 X は P_1, P_2, \dots, P_m のいずれによっても割り切れない。すなわち、 X が m 個の小さな素数 P_1, P_2, \dots, P_m を素因数に持たないということになり、 X が素数である確率は、単に無作為に生成した整数が素数である確率よりも高くなる。

【0029】そして、上記連立1次合同式の解 X は、 $X = a_1 (P_1 P_2 \dots P_m / P_1) B_1 + a_2 (P_1 P_2 \dots P_m / P_2) B_2 + \dots + a_m (P_1 P_2 \dots P_m / P_m) B_m \pmod{P_1 P_2 \dots P_m}$ によって簡単に求められることが知られており、第1の演算手段4はこの式、すなわち【数1】により整数 X を算出する。

【0030】このように本実施の形態では、乱数発生器が1つの整数を無作為に生成すると、その整数をもとに所定の演算式(【数1】)にしたがって素数である確率の高い整数、すなわち素数の候補が必ず1つ生成される。したがって、従来のように無作為に多数の整数を生成して素数を選別する方式に比べ極めて短時間で素数の候補を得ることができる。また、従来は素数であるか否かを調べるために除算を行う必要があったが、本実施の形態では除算は不要であり、したがって、除算器を用いることなく低コストで装置を構成することができる。

【0031】なお、加算器107が、剰余演算器106からの整数 X に $Q P_1 P_2 \dots P_m$ を加算する結果、加算器107が出力する n ビットの素数の候補(擬似乱数)は、 $\{2^{n-1}, \dots, 2^n - 1\}$ の上を一樣に分布するのではなく、 $\{Q P_1 P_2 \dots P_m, \dots, (Q+1) P_1 P_2 \dots P_m - 1\}$ の上を一樣に分布することになる。したがって、この n ビットの素数の候補は、統計的には理想的な擬似乱数とは言えないが、本実施の形態では生成した素数の候補を公開鍵暗号の秘密鍵を得るために利用するので、このような場合には十分である。

【0032】次に、第2の実施の形態について説明する。図2は本発明による擬似乱数発生装置の第2の実施の形態を示す機能ブロック図である。以下ではこの図を参照して本発明による擬似乱数発生装置の第2の実施の形態について説明し、同時に、対応する本発明による擬似乱数発生方法の実施の形態について説明する。なお、図2中、図1と同一の要素には同一の符号が付されており、それらに関する説明はここでは省略する。

【0033】この擬似乱数発生装置6が図1の擬似乱数発生装置2と異なるのは、図1の乱数発生器101が複数の乱数発生器201_kにより置き換えられ、そして、第1の演算手段4に相当する第1の演算手段5において

各除算器102_kが削除されている点である。すなわち、この擬似乱数発生装置6では、各加算器103_kに対応して乱数発生器201_kが設けられ、各乱数発生器201_kには入力端子180を通じてクロック信号が入力され、また、各乱数発生器201_kに対応する入力端子290_kを通じて整数 $(P_k - 1)$ が供給されている。そして、各乱数発生器201_kは、クロック信号の各クロックパルスが入力されるごとに、 $0 \leq A_k < (P_k - 1)$ を満たす擬似乱数 A_k を生成し、対応する加算器103_kに出力する。そして、この擬似乱数発生装置6では、各乱数発生器201_kが、上記除算器102_k(図1)が出力する整数 $D_k \bmod (P_k - 1)$ に相当する擬似乱数 A_k を生成し、加算器103_k以降の各部は上記実施の形態の場合と同様に動作して、 n ビットの整数を素数の候補として生成する。したがって、この実施の形態でも、上記実施の形態の場合と同様の効果が得られ、さらに、この実施の形態では乱数発生器の数は増すものの、 m 個の除算器が不要になるので、上記実施の形態より一層高速に素数の候補を生成することができる。

【0034】次に、第3の実施の形態について説明する。図3は本発明による擬似乱数発生装置の第3の実施の形態を示す機能ブロック図である。以下ではこの図を参照して本発明による擬似乱数発生装置の第3の実施の形態について説明し、同時に、対応する本発明による擬似乱数発生方法の実施の形態について説明する。なお、図3中、図2と同一の要素には同一の符号が付されており、それらに関する説明はここでは省略する。

【0035】この擬似乱数発生装置8が図2の擬似乱数発生装置6と異なるのは、図2の各乗算器104_kがそれぞれROM(リード・オンリ・メモリ)301_kにより置き換えられ、また、剰余演算器106が、加算器303₁、303₂およびROM302₁、302₂により置き換えられている点である。まず、各ROM301_kのアドレス端子には各加算器103_kの加算結果が入力され、各ROM301_kのデータ出力端子からは各ROM301_kが保持しているデータが加算器105に供給されている。そして、各ROM301_kの y 番地には(y は非負整数)、整数 $a_k (P_1 P_2 \dots P_m / P_k) y$ の値がデータとして書き込まれており、したがって、各ROM301_kは各乗算器104_kと同じ機能を果たす。各加算器103_kから各ROM301_kに入力されるのは整数 B_k であり、この値は小さい。したがって、各ROM301_kのアドレスの最大値も小さくてよく、記憶容量の小さいROMを用いることができるので、このような構成は容易に実現できる。

【0036】一方、加算器105の出力データを構成する複数のビットのうち、下位側の n ビットは加算器303₁の一方の入力端子に、残りのビットはROM302₁のアドレス端子にそれぞれ供給され、ROM302₁の出力データは加算器303₁のもう一方入力端子に供給

されている。また、加算器3031の出力データを構成する複数のビットのうち、下位側の n ビットは加算器3032の一方の入力端子に、残りのビットはROM3022のアドレス端子にそれぞれ供給され、ROM3022の出力データは加算器3032のもう一方入力端子に供給されている。

【0037】そして、各ROM3021、3022の z 番地 (z は非負整数) に、整数 $2^nz \pmod{P_1P_2\cdots P_m}$ の値がデータとして書き込まれており、その結果、これら加算器3031、3032およびROM3021、3023は剰余演算器106の機能を果たし、加算器3032からは整数 X が出力される。各ROM3021、3022に入力される整数 z は高々 m であり、 m の値は小さいので、記憶容量の小さいROMを用いることができ、このような構成は容易に実現できる。

【0038】この第3の実施の形態では、上述した擬似乱数発生装置6の場合と同様の効果が得られ、さらに、乗算器および剰余演算器を用いないので、さらに高速に素数の候補を生成することができる。なお、この第3の実施の形態では、第2の実施の形態を構成する乗算器および剰余演算器をROMや加算器で置き換えたが、第1の実施の形態においても同様に乗算器および剰余演算器をROMや加算器で置き換え、処理の高速化を図ることも無論可能である。

【0039】

【発明の効果】以上説明したように本発明の擬似乱数発生方法は、 m を正の整数、 P_1, P_2, \dots, P_m を2以上の素数として、与えられた整数 $(P_1-1)(P_2-1)\cdots(P_m-1)$ にもとづき、 $0 \leq A < (P_1-1)(P_2-1)\cdots(P_m-1)$ を満たす擬似乱数 A を乱数発生手段により生成する乱数発生ステップと、 D_k を $D_1=A$ で2以上 m 以下の整数 k に対して式 $D_k = D_{k-1} / (P_k-1)$ により表される整数、 B_k を m 以下の正の整数 k に対して式 $\{D_k \bmod (P_k-1)\} + 1$ により表される複数の整数、ならびに a_k を合同式 $a_k(P_1P_2\cdots P_m/P_k) = 1 \pmod{P_k}$ を満たす複数の整数として、式 $a_1(P_1P_2\cdots P_m/P_1)B_1 + a_2(P_1P_2\cdots P_m/P_2)B_2 + \cdots + a_m(P_1P_2\cdots P_m/P_m)B_m \pmod{P_1P_2\cdots P_m}$ により表される整数 X を剰余演算手段、加算手段、ならびに乗算手段を用いて算出する第1の演算ステップと、 n を正の整数、 Q を条件 $2^{n-1} \leq QP_1P_2\cdots P_m$ および $(Q+1)P_1P_2\cdots P_m \leq 2^n$ を満たす整数として、加算手段により前記整数 X に整数 $QP_1P_2\cdots P_m$ を加算して整数を生成し、出力する第2の演算ステップと、を含むことを特徴とする。

【0040】また、本発明の擬似乱数発生装置は、 m を正の整数、 P_1, P_2, \dots, P_m を2以上の素数として、入力された整数 $(P_1-1)(P_2-1)\cdots(P_m-1)$ にもとづいて、 $0 \leq A < (P_1-1)(P_2-1)\cdots(P_m-1)$ を満たす擬似乱数 A を生成する乱数発生手段と、 D_k を $D_1=A$ で2以上 m 以下の整数 k に対して式 $D_k = D_{k-1} / (P_k-1)$ により表される整数、 B_k を m 以下の正の整数 k に対して式 $\{D_k \bmod (P_k-1)\} + 1$ により表される複数の整数、ならびに a_k を合同式 $a_k(P_1P_2\cdots P_m/P_k) = 1 \pmod{P_k}$ を満たす複数の整数として、式 $a_1(P_1P_2\cdots P_m/P_1)B_1 + a_2(P_1P_2\cdots P_m/P_2)B_2 + \cdots + a_m(P_1P_2\cdots P_m/P_m)B_m \pmod{P_1P_2\cdots P_m}$ により表される整数 X を剰余演算手段、加算手段、ならびに乗算手段を含む第1の演算手段と、 n を正の整数、 Q を条件 $2^{n-1} \leq QP_1P_2\cdots P_m$ および $(Q+1)P_1P_2\cdots P_m \leq 2^n$ を満たす整数として、前記整数 X に整数 $QP_1P_2\cdots P_m$ を加算して整数を生成し、出力する第2の演算手段と、を含むことを特徴とする。

…… (P_m-1) を満たす擬似乱数 A を生成する乱数発生手段と、 D_k を $D_1=A$ で2以上 m 以下の整数 k に対して式 $D_k = D_{k-1} / (P_k-1)$ により表される整数、 B_k を m 以下の正の整数 k に対して式 $\{D_k \bmod (P_k-1)\} + 1$ により表される複数の整数、ならびに a_k を合同式 $a_k(P_1P_2\cdots P_m/P_k) = 1 \pmod{P_k}$ を満たす複数の整数として、式 $a_1(P_1P_2\cdots P_m/P_1)B_1 + a_2(P_1P_2\cdots P_m/P_2)B_2 + \cdots + a_m(P_1P_2\cdots P_m/P_m)B_m \pmod{P_1P_2\cdots P_m}$ により表される整数 X を算出する、剰余演算手段、加算手段、ならびに乗算手段を含む第1の演算手段と、 n を正の整数、 Q を条件 $2^{n-1} \leq QP_1P_2\cdots P_m$ および $(Q+1)P_1P_2\cdots P_m \leq 2^n$ を満たす整数として、前記整数 X に整数 $QP_1P_2\cdots P_m$ を加算して整数を生成し、出力する第2の演算手段と、を含むことを特徴とする。

【0041】すなわち、本発明では、擬似乱数 A より所定の数式にもとづいて、素数である確率の高い整数 X を算出するので、1つの擬似乱数 A に対して、素数の候補が必ず1つ生成される。したがって、従来のように無作為に多数の整数を生成して素数を選別する方式に比べ極めて短時間で素数の候補を得ることができる。また、従来は素数であるか否かを調べるために除算を行う必要があったが、本発明では除算は不要であり、したがって、除算器を用いることなく低コストで装置を構成することができる。

【0042】さらに、本発明の擬似乱数発生方法は、 m を正の整数、 k を m 以下の正の整数、 P_1, P_2, \dots, P_m を2以上の素数として、与えられた複数の整数 $(P_1-1), (P_2-1), \dots, (P_m-1)$ にもとづき、 $0 \leq A_k < (P_k-1)$ を満たす複数の擬似乱数 A_k を、複数の乱数発生手段によりそれぞれ生成する乱数発生ステップと、 B_k を式 $A_k + 1$ により表される複数の整数、ならびに a_k を合同式 $a_k(P_1P_2\cdots P_m/P_k) = 1 \pmod{P_k}$ を満たす複数の整数として、式 $a_1(P_1P_2\cdots P_m/P_1)B_1 + a_2(P_1P_2\cdots P_m/P_2)B_2 + \cdots + a_m(P_1P_2\cdots P_m/P_m)B_m \pmod{P_1P_2\cdots P_m}$ により表される整数 X を剰余演算手段、加算手段、ならびに乗算手段を用いて算出する第1の演算ステップと、 n を正の整数、 Q を条件 $2^{n-1} \leq QP_1P_2\cdots P_m$ および $(Q+1)P_1P_2\cdots P_m \leq 2^n$ を満たす整数として、加算手段により前記整数 X に整数 $QP_1P_2\cdots P_m$ を加算して整数を生成し、出力する第2の演算ステップと、を含むことを特徴とする。

【0043】また、本発明の擬似乱数発生装置は、 m を正の整数、 k を m 以下の正の整数、 P_1, P_2, \dots, P_m を2以上の素数として、入力された複数の整数 $(P_1-1), (P_2-1), \dots, (P_m-1)$ にもとづいて $0 \leq A_k < (P_k-1)$ を満たす複数の擬似乱数 A_k をそれぞれ生成する複数の乱数発生手段と、 B_k を式 $A_k + 1$ に

より表される前記複数の整数、ならびに a_k を合同式 $a_k (P_1 P_2 \cdots P_m / P_k) = 1 \pmod{P_k}$ を満たす複数の整数として、式 $a_1 (P_1 P_2 \cdots P_m / P_1) B_1 + a_2 (P_1 P_2 \cdots P_m / P_2) B_2 + \cdots + a_m (P_1 P_2 \cdots P_m / P_m) B_m \pmod{P_1 P_2 \cdots P_m}$ により表される整数 X を算出する、剰余演算手段、加算手段、ならびに乗算手段を含む第1の演算手段と、 n を正の整数、 Q を条件 $2^{n-1} \leq Q P_1 P_2 \cdots P_m$ および $(Q+1) P_1 P_2 \cdots P_m \leq 2^n$ を満たす整数として、前記整数 X に整数 $Q P_1 P_2 \cdots P_m$ を加算して整数を生成し、出力する第2の演算手段と、を含むことを特徴とする。

【0044】すなわち、本発明では、複数の擬似乱数 A_k より所定の数式にもとづいて、素数である確率の高い整数 X を算出するので、1組みの擬似乱数 A_k に対して、素数の候補が必ず1つ生成される。したがって、従来のように無作為に多数の整数を生成して素数を選別する方式に比べ極めて短時間で素数の候補を得ることができる。また、従来は素数であるか否かを調べるために除算を行う必要があったが、本発明では除算は不要であ

り、したがって、除算器を用いることなく低コストで装置を構成することができる。

【図面の簡単な説明】

【図1】本発明による擬似乱数発生装置の一実施の形態を示す機能ブロック図である。

【図2】本発明による擬似乱数発生装置の第2の実施の形態を示す機能ブロック図である。

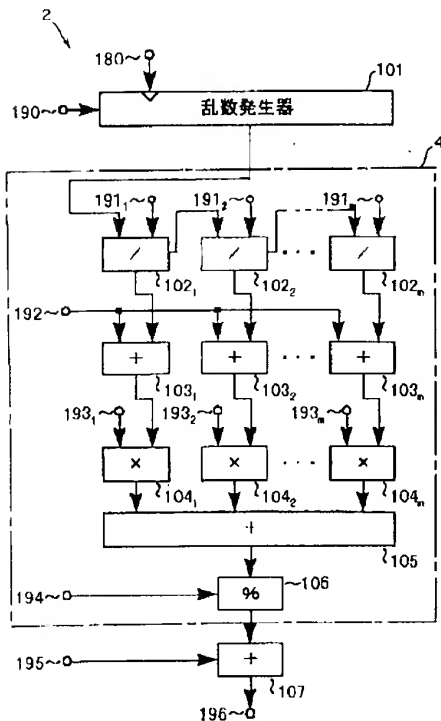
【図3】本発明による擬似乱数発生装置の第3の実施の形態を示す機能ブロック図である。

【図4】従来の素数の候補を生成する方法を示すフローチャートである。

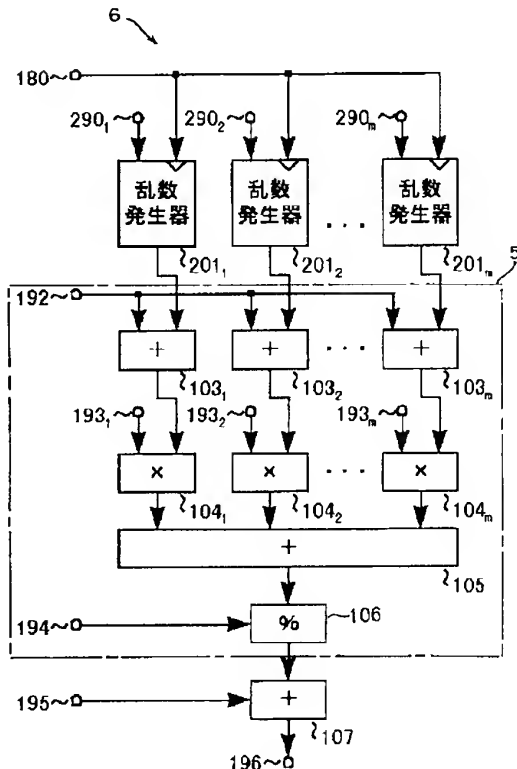
【符号の説明】

2、6、8……擬似乱数発生装置、4、5……第1の演算手段、101、201₁、201₂、201_m……乱数発生器、105、107、103₁、103₂、103_m、302₁、303₂……加算器、106、102₁、102₂、102_m……剰余演算器、104₁、104₂、104_m……乗算器、301₁、301₂、301_m、302₁、302₂……ROM（リード・オンリ・メモリ）。

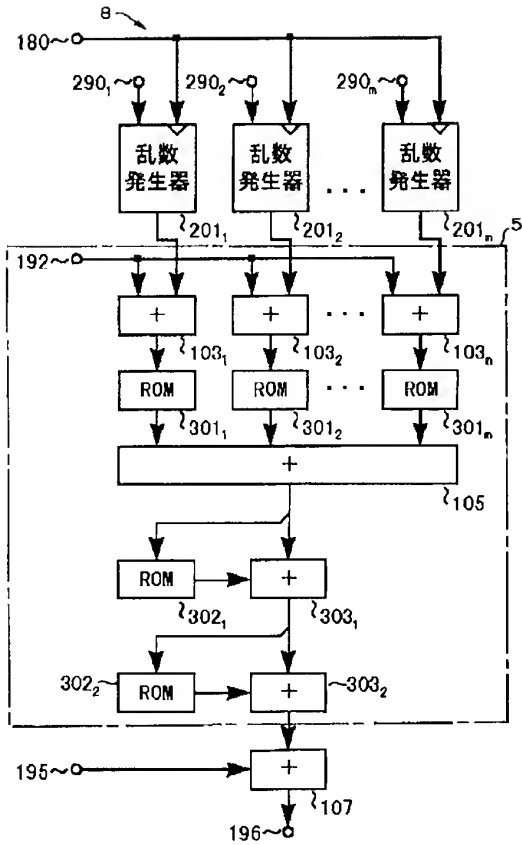
【図1】



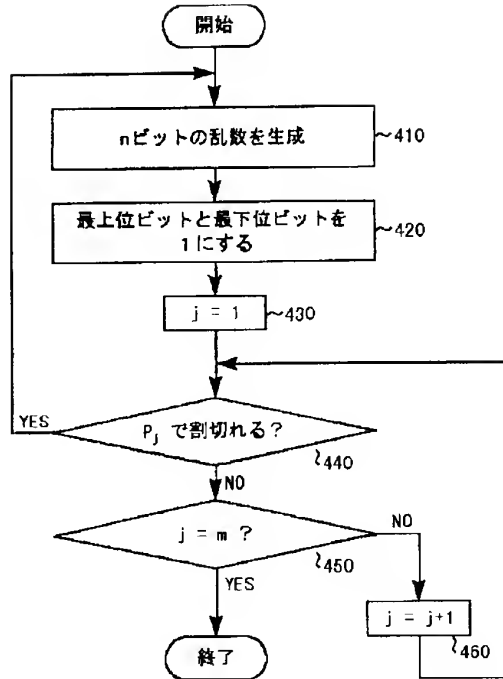
【図2】



【図3】



【図4】



PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-109859

(43)Date of publication of application : 23.04.1999

(51)Int.Cl. G09C 1/00
G06F 7/58

(21)Application number : 09-290350 (71)Applicant : NEC CORP
(22)Date of filing : 06.10.1997 (72)Inventor : SHIMADA MICHIO

(54) METHOD FOR GENERATING PSEUDO-RANDOM NUMBER

(57)Abstract:

PROBLEM TO BE SOLVED: To generate an integer which is to be a candidate of a prime number at a low cost in a short time.

SOLUTION: A random number generation unit 101 generates an integer A at random which satisfies $0 \leq A < (P_1-1)(P_2-1) \dots (P_m-1)$ synchronizing with the clock pulse from input terminal 180. P_1, P_2, \dots and P_m are prime numbers of two or more. A first operation means 4 calculates an integer X a prime number with a high probability from this integer A based on an expression

$$X = a_1(P_1 P_2 \dots P_m / P_1) B_1 + a_2(P_1 P_2 \dots P_m / P_2) B_2 + \dots + a_m(P_1 P_2 \dots P_m / P_m) B_m \pmod{P_1 P_2 \dots P_m}$$
However, $a_k (k=1, 2, \dots, m)$ is an integer l satisfying a congruence expression $a_k(P_1 P_2 \dots P_m / P_k) = 1 \pmod{P_k}$ and B_r expresses $[A \bmod (P_k-1)] + 1$. An adder 107 outputs the integer X as an integer of a specific number of bits.

CLAIMS

[Claim(s)]

[Claim 1] A pseudorandom-numbers generation method comprising:

For m a positive integer P_1, P_2, \dots, P_m as two or more prime numbers A random number generation step which generates the pseudorandom numbers A which fill $0 \leq A < (P_1-1)(P_2-1) \dots (P_m-1)$ by a random number generation means based on given integer $(P_1-1)(P_2-1) \dots (P_m-1)$.

Two or more integers expressed with $D_1=A$ by formula $D_k = D_{k-1} / (P_k-1)$ to the integer k below or more $2m$ in D_k Two or more integers expressed by formula $[D_k \bmod (P_k-1)] + 1$ to positive integer k below m in B_k And as two or more integers with which congruence

expression $a_k(P_1P_2 \dots P_m/P_k) \equiv 1 \pmod{P_k}$ is filled
 Formula $a_1(P_1P_2 \dots P_m/P_1) B_1 + a_2(P_1P_2 \dots P_m/P_2) B_2 + \dots + a_m(P_1P_2 \dots P_m/P_m) B_m \pmod{P_1P_2 \dots P_m}$
 The 1st arithmetic step that computes the integer X expressed by P_m using a division means
 a remainder arithmetic means an adding means and a multiplication means
 A positive integer Q Condition $2^{n-1} \leq QP_1P_2 \dots P_m$ and $(Q+1)P_1P_2 \dots P_m$
 It is integer $QP_1P_2 \dots P_m$ to said integer X by an adding means
 as an integer with which $P_m \leq 2^n$ is filled.... The 2nd arithmetic step that adds P_m generates an integer and is outputted

[Claim 2] The pseudorandom-numbers generation method comprising according to claim 1:

Said 1st arithmetic step A division step which computes quotient $D_{k+1} = D_k / (P_k - 1)$ when it is referred to as $D_1 = A$ and integer D_k is $**(\text{ed})$ for an integer $(P_k - 1)$ to the integer k below or more 2 and surplus $D_k \pmod{(P_1 - 1)}$ by a division means.

The 1st summing step that adds 1 to each of a surplus computed at said division step by the 1st adding means and computes said two or more integer B_k respectively.

A multiplication step which multiplies by integer $a_k(P_1P_2 \dots P_m/P_k)$ which uses said multiplication means for each of two or more of said integer B_k computed by said 1st summing step and corresponds to it.

The 2nd summing step that adds a multiplication result in this multiplication step altogether by the 2nd adding means It is an added result in this 2nd summing step
 Integer $P_1P_2 \dots P_m$ A remainder arithmetic step which computes a surplus when it $**$ by P_m by a remainder arithmetic means and is made into said integer X

[Claim 3] A pseudorandom-numbers generation method comprising:

A positive integer below $mP_1P_2 \dots P_m$ and P_m for a positive integer and k as two or more prime numbers [m] being based on two or more given integers $(P_1 - 1)(P_2 - 1) \dots$ and $(P_m - 1) - 0 \leq A_k < (P_k - 1)$ -- a random number generation step which generates two or more pseudorandom-numbers A_k to fill by two or more random number generation means respectively.

Two or more integers expressed by formula $A_k + 1$ in B_k and a_k as two or more integers with which congruence expression $a_k(P_1P_2 \dots P_m/P_k) \equiv 1 \pmod{P_k}$ is filled
 Formula $a_1(P_1P_2 \dots P_m/P_1) B_1 + a_2(P_1P_2 \dots P_m/P_2) B_2 + \dots + a_m(P_1P_2 \dots P_m/P_m) B_m \pmod{P_1P_2 \dots P_m}$

The 1st arithmetic step that computes the integer X expressed by P_m using a remainder arithmetic means an adding means and a multiplication means They are a positive integer and Q about n Condition $2^{n-1} \leq QP_1P_2 \dots P_m$ and $(Q+1)P_1P_2 \dots P_m$ as an integer with which $P_m \leq 2^n$ is filled It is integer $QP_1P_2 \dots P_m$ to said integer X by an adding means.... The 2nd arithmetic step that adds P_m generates an integer and is outputted

[Claim 4] The pseudorandom-numbers generation method comprising according to claim 3:

The 1st summing step that said 1st arithmetic step adds 1 to each of two or more of said pseudorandom-numbers A_k generated at said random number generation step by the 1st adding means and computes said two or more integer B_k respectively.

A multiplication step which multiplies by integer $a_k (P_1 P_2 \dots P_m / P_k)$ which uses said multiplication means for each of two or more of said integer B_k computed by said 1st summing step and corresponds to it.

The 2nd summing step that adds a multiplication result in this multiplication step altogether by the 2nd adding means.

It is an added result in this 2nd summing step Integer $P_1 P_2 \dots$. The 2nd remainder arithmetic step that computes a surplus when it $**$ by P_m by a remainder arithmetic means and is made into said integer X

[Claim 5] A pseudorandom-numbers generator comprising:

For m a positive integer $P_1 P_2 \dots P_m$ as two or more prime numbers A random number generation means to generate the pseudorandom numbers A which fill $0 \leq A < (P_1 - 1) (P_2 - 1) \dots (P_m - 1)$ based on inputted integer $(P_1 - 1) (P_2 - 1) \dots (P_m - 1)$.

Two or more integers expressed with $D_1 = A$ by formula $D_k = D_{k-1} / (P_k - 1)$ to the integer k below or more $2m$ in D_k It is a formula to positive integer k below m about $B_k \{D_k \bmod (P_k - 1)\}$ Two or more integers expressed by $+1$ And as two or more integers with which

congruence expression $a_k (P_1 P_2 \dots P_m / P_k) = 1 \pmod{P_k}$ is filled a_k Formula $a_1 (P_1 P_2 \dots P_m / P_1) B_1 + a_2 (P_1 P_2 \dots P_m / P_2) B_2 + \dots + a_m (P_1 P_2 \dots P_m / P_m) B_m \pmod{P_1 P_2 \dots P_m}$ The 1st calculating means including a division means a remainder arithmetic means an adding means and a multiplication means which compute the integer X expressed by P_m They are a positive integer and Q about n Condition $2^{n-1} \leq Q P_1 P_2 \dots P_m$ and $(Q+1) P_1 P_2 \dots P_m$ as an integer with which $P_m \leq 2^n$ is filled. It is integer $Q P_1 P_2 \dots P_m$ to said integer X ...

The 2nd calculating means that adds P_m generates an integer and is outputted

[Claim 6] The pseudorandom-numbers generator comprising according to claim 5:

Said 1st calculating means is set to $D_1 = A$ to said pseudorandom numbers A Two or more division means which compute quotient $D_{k+1} = D_k / (P_k - 1)$ when integer D_k is $**$ (ed) for an integer $(P_k - 1)$ to the integer k below or more $2m$ and surplus $D_k \bmod (P_k - 1)$ by a division means.

Two or more 1st adding means that add 1 to each of a surplus computed by said 1st remainder arithmetic means and compute said two or more integer B_k respectively.

Said two or more multiplication means which multiply by integer $a_k (P_1 P_2 \dots P_m / P_k)$ corresponding to each of two or more of said integer B_k computed by said 1st adding means.

It is an added result by the 2nd adding means adding all multiplication results by this multiplication means and this 2nd adding means Integer $P_1 P_2 \dots$ A remainder arithmetic means to compute a surplus when it $**$ by P_m and to output as said integer X

[Claim 7] A pseudorandom-numbers generator comprising:

A positive integer below $mP_1P_2\text{---}\text{---}$ and P_m for a positive integer and k as two or more prime numbers $[m]$ being based on two or more integers (P_1-1) and (P_2-1) which were inputted $\text{---}\text{---}$ and $(P_m-1) \text{---}$ $0 \leq A_k \text{---} < (P_k-1) \text{---}$ two or more random number generation means to generate two or more pseudorandom-numbers A_k to fill respectively.

Two or more integers expressed by formula A_k+1 in B_k and a_k as two or more integers with which congruence expression $a_k(P_1P_2\text{---}\text{---} P_m/P_k) \equiv 1 \pmod{P_k}$ is filled Formula $a_1(P_1P_2\text{---}\text{---} P_m/P_1) B_1 + a_2(P_1P_2\text{---}\text{---} P_m/P_2) B_2 + \dots + a_m(P_1P_2\text{---}\text{---} P_m/P_m) B_m \pmod{P_1P_2\text{---}\text{---}}$. The 1st calculating means including a remainder arithmetic means an adding means and a multiplication means which compute the integer X expressed by P_m . They are a positive integer and Q about n . Condition $2^{n-1} \leq QP_1P_2\text{---}\text{---} P_m$ and $(Q+1) P_1P_2\text{---}\text{---}$ as an integer with which $P_m \leq 2^n$ is filled. It is integer QP_1P_2 to said integer X . The 2nd calculating means that adds P_m generates an integer and is outputted.

[Claim 8] The pseudorandom-numbers generator comprising according to claim 7:

Two or more 1st adding means that said 1st calculating means adds 1 to each of two or more of said pseudorandom-numbers A_k generated by said random number generation means and compute said two or more integer B_k respectively.

Said two or more multiplication means which multiply by integer $a_k(P_1P_2\text{---}\text{---} P_m/P_k)$ corresponding to each of two or more of said integer B_k computed by said 1st adding means.

The 2nd adding means adding all multiplication results in this multiplication means.

It is an added result in this 2nd adding means Integer $P_1P_2\text{---}\text{---}$. A remainder arithmetic means to compute a surplus when it $**$ by P_m and to output as said integer X .

[Claim 9] The pseudorandom-numbers generator according to claim 6 or 8 wherein said multiplication means is constituted by ROM.

[Claim 10] The aforementioned remainder arithmetic means contains the 1st and 2nd ROM and 1st and 2nd adding machines. Two or more bits by the side of a low rank are supplied to one input terminal of said 1st adding machine among two or more bits which constitute output data of said 2nd adding means. The remaining bits are supplied to an address terminal of said 1st ROM and output data of said 1st ROM is supplied to an another side input terminal of said 1st adding machine. Inside of two or more of said bits which constitute output data of said 1st adding machine. Two or more bits by the side of a low rank are supplied to one input terminal of said 2nd adding machine. The remaining bits are supplied to an address terminal of said 2nd ROM and output data of said 2nd ROM is supplied to an another side input terminal of said 2nd adding machine. The pseudorandom-numbers generator according to claim 6 or 8 wherein output data of said 2nd adding machine is outputted as a computed result of said

surplus of the aforementioned remainder arithmetic means.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the method and device which generate pseudorandom numbers.

[0002]

[Description of the Prior Art] Before in order that the transmitted data in communications systems such as a telephone, a modem, or television may not be intercepted by the third party, encryption of transmit information is performed to transmit information by carrying out exclusive OR addition of the pseudorandom numbers. Two art of the public key encryption using a key which is different by the conventional code using the same key and encryption and decryption by encryption and decryption to the method of encryption is known. Among these since time and effort can be saved since the public-key crypto system does not need to deliver a key beforehand in advance of communication and what is necessary is to perform management of a key only by a receiver it has the advantage that management of a key is easy.

[0003] In a public-key crypto system a receiver decrypts information using a secret key and the prime number which usually has a thousands of [hundreds to] bits. A prime number is used for this secret key. Therefore it has been an important technical problem how a prime number with much such the number of bits is generated efficiently random.

[0004] When generating the prime number of the specific number of bits fundamentally the integer of the number of specific bits is generated at random first and it is necessary to repeat since a formula does not exist in generation of such a prime number until a prime number is obtained [judging whether it is a prime number and]. However since a lot of [in order to judge whether it is a prime number] calculations were required shortening of time was aimed at by generating first an integer with probability high as a candidate of a prime number which is a prime number rather than only generating the integer of the number of specific bits at random and judging conventionally that it is a prime number to the integer.

[0005] Drawing 4 is a flow chart which shows how to generate the candidate of such a conventional prime number. As shown in this figure the integer X (pseudorandom numbers) of n bit is first generated at random by making n into a positive integer (Procedure 410). However since there is the integer X clearly again not a prime number but when a high order bit is not an n bit because of zero if the integer X is even the least significant bit and the most significant bit of the integer X are set to 1 (Procedure 420). Next positive integer j is set to 1 (Procedure 430) and it inspects

whether X can divide among P_j when X can divide among P_j , control is moved to Procedure 410 and on the other hand when it cannot be divided, control is moved to Procedure 450. In Procedure 450 it inspects whether it is $j=m$. If $j=m$, processing will be ended. X will be outputted as a candidate (pseudorandom numbers) of a prime number and if it is not $j=m$, control will be moved to Procedure 460. In Procedure 460 it is considered as $j=j+1$ and control is moved to 440. m is the positive integer decided beforehand here and P_m is P_1, P_2, \dots , a mutually different small prime number. Since P_1, P_2, \dots having P_m in a prime factor will not have X if it carries out for coming and the integer X is generated rather than the integer of n bit generated at random simply, the probability which is a prime number becomes high and the prime number of the number of specific bits can be obtained efficiently.

[0006] About the conventional prime-number-generation method and public key encryption. For example, SHUNAI work "applied cryptography (2nd edition)" ()

[Bruce Schneier and] Applied Cryptography: It explains to Protocols, Algorithms and Source Code in C Second Edition John Wiley & Sons Inc. 1996 etc. in detail.

[0007]

[Problem(s) to be Solved by the Invention] However, the probability that the integer of n bit generated at random is a prime number is about $1/n$ considering a prime number theorem. It is known that it is a grade. Therefore, in the conventional method, in order to obtain the candidate of one prime number, about n integers needed to be generated at random. And since the prime number of thousands of [hundreds to] numbers of bits is used as mentioned above as a secret key, in order to obtain one candidate of such a secret key, it had to check whether the integer which generated the integer also thousands times from hundreds of times and was generated at every time would be \times (ed) by prime number P_j and an integer could divide among P_j and a lot of operations needed to be performed. Therefore, in order to take time in order to obtain the candidate of a prime number and to do division, a divider is required and the device had become a high cost.

[0008] Then the purpose of this invention is to provide the pseudorandom-numbers generation method and device which are short time and can generate the integer which serves as a candidate of a prime number by low cost.

[0009]

[Means for Solving the Problem] A pseudorandom-numbers generation method of this invention for m a positive integer P_1, P_2, \dots, P_m in order to attain the above-mentioned purpose as two or more prime numbers. Based on given integer $(P_1-1) (P_2-1) \dots (P_m-1)$, a random number generation step which generates the pseudorandom numbers A which fill $0 \leq A < (P_1-1) (P_2-1) \dots (P_m-1)$ by a random number generation means. Two or more integers expressed with $D_1=A$ by formula $D_k=D_{k-1}/(P_k-1)$ to the integer k below or more $2m$ in D_k . Two or more integers expressed by formula $\{D_k \bmod (P_k-1)\}+1$ to positive integer k below m in B_k . And as two or more integers with which congruence expression $a_k(P_1 P_2 \dots P_m / P_k) = 1 \pmod{P_k}$ is filled, a_k . Formula $a_1, (P_1 P_2 \dots P_m / P_1)$

$B_1 + a_2(P_1 P_2 \dots P_m / P_2) B_2 + \dots + a_m(P_1 P_2 \dots P_m / P_m) B_m \pmod{P_1 P_2 \dots}$ The 1st arithmetic step that computes the integer X expressed by P_m using a division means a remainder arithmetic means an adding means and a multiplication means They are a positive integer and Q about n Condition $2^{n-1} \leq Q P_1 P_2 \dots P_m$ and $(Q+1) P_1 P_2 \dots$ as an integer with which $P_m \leq 2^n$ is filled It is integer $Q P_1 P_2$ to said integer X by an adding means.... P_m is added an integer is generated and the 2nd arithmetic step to output is included.

[0010] A pseudorandom-numbers generation method of this invention is provided with the following.

A positive integer below $m P_1 P_2 \dots$ and P_m for a positive integer and k as two or more prime numbers [m] being based on two or more given integers $(P_1-1)(P_2-1) \dots$ and $(P_m-1) - 0 \leq A_k < (P_k-1)$ - a random number generation step which generates two or more pseudorandom-numbers A_k to fill by two or more random number generation means respectively.

Two or more integers expressed by formula $A_k + 1$ in B_k and a_k as two or more integers with which congruence expression $a_k(P_1 P_2 \dots P_m / P_k) = 1 \pmod{P_k}$ is filled Formula $a_1 \cdot (P_1 P_2 \dots P_m / P_1) B_1 + a_2(P_1 P_2 \dots P_m / P_2) B_2 + \dots + a_m(P_1 P_2 \dots P_m / P_m) B_m \pmod{P_1 P_2 \dots}$

The 1st arithmetic step that computes the integer X expressed by P_m using a remainder arithmetic means an adding means and a multiplication means They are a positive integer and Q about n Condition $2^{n-1} \leq Q P_1 P_2 \dots P_m$ and $(Q+1) P_1 P_2 \dots$ as an integer with which $P_m \leq 2^n$ is filled It is integer $Q P_1 P_2$ to said integer X by an adding means.... The 2nd arithmetic step that adds P_m generates an integer and is outputted

[0011] And a pseudorandom-numbers generator of this invention is provided with the following.

For m a positive integer $P_1 P_2 \dots P_m$ as two or more prime numbers A random number generation means to generate the pseudorandom numbers A which fill $0 \leq A < (P_1-1)(P_2-1) \dots (P_m-1)$ based on inputted integer $(P_1-1)(P_2-1) \dots (P_m-1)$.

Two or more integers expressed with $D_1 = A$ by formula $D_k = D_{k-1} / (P_k - 1)$ to the integer k below or more $2m$ in D_k It is a formula to positive integer k below m about $B_k \{D_k \pmod{P_k - 1}\}$ Two or more integers expressed by +1 And as two or more integers with which

congruence expression $a_k(P_1 P_2 \dots P_m / P_k) = 1 \pmod{P_k}$ is filled a_k Formula $a_1 \cdot (P_1 P_2 \dots P_m / P_1) B_1 + a_2(P_1 P_2 \dots P_m / P_2) B_2 + \dots + a_m(P_1 P_2 \dots P_m / P_m) B_m \pmod{P_1 P_2 \dots}$ The 1st calculating means including a division means a remainder arithmetic means an adding means and a multiplication means which compute the integer X expressed by P_m

They are a positive integer and Q about n Condition $2^{n-1} \leq Q P_1 P_2 \dots P_m$ and $(Q+1) P_1 P_2 \dots$ as an integer with which $P_m \leq 2^n$ is filled It is integer $Q P_1 P_2$ to said integer X.... The 2nd calculating means that adds P_m generates an integer and is outputted

[0012] A pseudorandom-numbers generator of this invention is provided with the

following.

A positive integer below $mP_1P_2\cdots$ and P_m for a positive integer and k as two or more prime numbers $[m]$ being based on two or more integers (P_1-1) and (P_2-1) which were inputted and $(P_m-1) \rightarrow 0 \leq A_k \rightarrow (P_k-1) \rightarrow$ two or more random number generation means to generate two or more pseudorandom-numbers A_k to fill respectively.

Said two or more integers expressed by formula A_k+1 in B_k And as two or more integers with which congruence expression $a_k(P_1P_2\cdots P_m/P_k) \equiv 1 \pmod{P_k}$ is filled a_k . Formula $a_1 \cdot (P_1P_2\cdots P_m/P_1) B_1 + a_2(P_1P_2\cdots P_m/P_2) B_2 + \cdots + a_m(P_1P_2\cdots P_m/P_m) B_m \pmod{P_1P_2\cdots}$. The 1st calculating means including a remainder arithmetic means an adding means and a multiplication means which compute the integer X expressed by P_m .

They are a positive integer and Q about n Condition $2^{n-1} \leq QP_1P_2\cdots P_m$ and $(Q+1)P_1P_2\cdots$ as an integer with which $P_m \leq 2^n$ is filled. It is integer QP_1P_2 to said integer X The 2nd calculating means that adds P_m generates an integer and is outputted

[0013] The above-mentioned integer B_k expressed with $\{D_k \bmod (P_k-1)+1\}$ fills $0 < B_k < P_k$ to given arbitrary nonnegative integer D_k . It is $B_k \neq 0$ if it is $0 < B_k < P_k \pmod{P_k}$. Therefore if it is $P_1P_2\cdots$ a prime number in which P_m is different. A primary alliance congruence expression If a solution of $X \equiv B_1 \pmod{P_1} X \equiv B_2 \pmod{P_2} \cdots X \equiv B_m \pmod{P_m}$ exists and the solution is set to X (the above-mentioned integer X) X can be divisible by neither P_1 nor P_2 nor \cdots nor P_m . That is small prime number $P_1P_2\cdots$ probability that X is a prime number become higher than probability that an integer given only at random $[X]$ it will be said that it does not have P_m in a prime factor and $[X]$ is a prime number.

[0014] And the solution X of the above-mentioned primary alliance congruence expression $X \equiv a_1 \cdot (P_1P_2\cdots P_m/P_1) B_1 + a_2(P_1P_2\cdots P_m/P_2) B_2 + \cdots + a_m(P_1P_2\cdots P_m/P_m) B_m \pmod{P_1P_2\cdots}$. Asking simply is known by P_m and the integer X is computed by this formula in the 1st arithmetic step of the above and the 1st calculating means in a pseudorandom-numbers generation method and a device of this invention which generate the one pseudorandom numbers A first. At the 2nd arithmetic step of the above and the 2nd calculating means it is QP_1P_2 to the integer X Since P_m is added an integer of n bit is acquired as the final output.

[0015] In this invention pseudorandom-numbers generation method and a device which generate two or more pseudorandom numbers A_k to the beginning. Pseudorandom-numbers A_k which is equivalent to above-mentioned $D_k \bmod (P_k-1)$ by random number generation step and a random number generation means is generated. In the 1st arithmetic step and 1st calculating means the integer X is computed by this pseudorandom-numbers A_k and the 2nd arithmetic step and 2nd calculating means generate an integer of n bit like a case of the above-mentioned invention further.

[0016]

[Embodiment of the Invention] Next an embodiment of the invention is described with reference to drawings. Drawing 1 is a functional block diagram showing the 1st embodiment of the pseudorandom-numbers generator by this invention. Below with reference to this figure the 1st embodiment of the pseudorandom-numbers generator by this invention is described and the 1st embodiment of the pseudorandom-numbers generation method by corresponding this invention is described simultaneously.

[0017] As it is for this pseudorandom-numbers generator 2 generating the candidate of the prime number used as the secret key of a public-key crypto system and was shown in drawing 1 it is constituted by the adding machine 107 as the random number generator 101 as a random number generation means concerning this invention, the 1st calculating means 4 concerning this invention and the 2nd calculating means concerning this invention. The 1st calculating means 4 And divider $102_1, 102_2, \dots, 102_m$ (division means concerning this invention), adding machine $103_1, 103_2, \dots, 103_m$ (the 1st adding means concerning this invention), multiplier $104_1, 104_2, \dots, 104_m$ (multiplication means concerning this invention), the adding machine 105 (the 2nd adding means concerning this invention) and the remainder arithmetic machine 106 (remainder arithmetic means concerning this invention).

[0018] a clock signal being supplied to the random number generator 101 through the input terminal 180 and leading the input terminal 190 to it on the other hand -- an integer $(P_1-1) (P_2-1) \dots (P_m-1)$ is inputted. Here a positive integer P_1, P_2, \dots, P_m of m are two or more prime numbers. And the random number generator 101 generates the pseudorandom numbers A which fill $0 \leq A < (P_1-1) (P_2-1) \dots (P_m-1)$ synchronizing with each clock pulse of the above-mentioned clock signal and outputs them to the 1st calculating means 4.

[0019] The function of the 1st calculating means 4 is computing the integer X (pseudorandom numbers) with high probability which is a prime number based on the next [one number].

[0020]

[Equation 1] $X = a_1 \cdot (P_1 P_2 \dots P_m / P_1) B_1 + a_2 (P_1 P_2 \dots P_m / P_2) B_2 + \dots + a_m (P_1 P_2 \dots P_m / P_m) B_m \pmod{P_1 P_2 \dots P_m}$

Here a_k ($k = 1, 2, \dots, m$) is an integer with which congruence expression $a_k (P_1 P_2 \dots P_m / P_k) \equiv 1 \pmod{P_k}$ is filled. B_1, B_2, \dots, B_m Formula type $B_k = \{D_k \pmod{(P_k-1)} + 1\}$ are two or more integers values are decided to be and here D_m is D_1, D_2, \dots and two or more integers values are decided to be by $D_k = D_{k-1} / (P_{k-1}-1)$ to $D_1 = A$ and two or more k . A reason for probability that the integer X expressed by [an one number] is a prime number being a high integer is explained in detail later.

[0021] An integer (P_k-1) is inputted into each divider 102_k ($k = 1, 2, \dots, m$) which constitutes the 1st calculating means 4 through terminal 191_k and the above-mentioned pseudorandom numbers A are inputted into divider 102_1 from the random number generator 101. And divider 102_1 computes quotient $D_2 = A / (P_1-1)$ when the pseudorandom numbers A are \div (ed) for an integer (P_1-1) and the surplus $A \pmod{(P_1-1)}$

1) Output a quotient and a surplus and each divider 102_k ($k=2\text{---}m$) Quotient $D_{k+1}=$ when quotient D_k which left-hand side divider 102_{k-1} outputs is \ast (ed) for an integer (P_k-1) ($D_k/(P_k-1)$) and surplus $D_k \bmod (P_k-1)$ are computed and a quotient and a surplus are outputted.) A surplus which each divider 102_k ($k=2\text{---}m$) outputs is outputted to each adding machine 103_k corresponding respectively. Below it is written as expedient upper $D_1=A$ of explanation. In each adding machine 103_k with the above-mentioned surplus from each divider 102_k , "1" is inputted through the input terminal 192 and each adding machine 103_k adds one to surplus $D_k \bmod (P_k-1)$. A result is outputted to each multiplier 104_k corresponding as integer $B_k (= \{D_k \bmod (P_k-1)\} + 1)$.

[0022] In each multiplier 104_k with added result B_k by each adding machine 103_k , Integer $a_k (P_1 P_2 \dots P_m / P_k)$ is inputted through each terminal 193, and multiplier 104_k computes a product of this integer and the above-mentioned added result B_k and outputs a result to the adding machine 105. a_k is an integer with which congruence expression $a_k (P_1 P_2 \dots P_m / P_k) \equiv 1 \pmod{P_k}$ is filled here. The adding machine 105 adds all outputs of each multiplier 104_k and outputs an added result to the remainder arithmetic machine 106. In the remainder arithmetic machine 106 with this added result through the terminal 194 Prime number $P_1 P_2 \dots$ integer $P_1 P_2$ as a product of $P_m \dots P_m$ is inputted. The remainder arithmetic machine 106 is an added result from the adding machine 105 Integer $P_1 P_2 \dots$. A surplus when it \ast by P_m is computed and it outputs to the adding machine 107 as the integer X .

[0023] The input terminal 195 is led to the adding machine 107 with the integer X from the remainder arithmetic machine 106 and it is the above-mentioned integer $P_1 P_2 \dots$. Integer $Q P_1 P_2$ which multiplied P_m by the integer $Q \dots P_m$ is inputted. The adding machine 107 outputs an integer (pseudorandom numbers) acquired by adding these integers as a candidate of a prime number used as a secret key. Here Q is condition $2^{n-1} \leq Q P_1 P_2 \dots P_m$ and $(Q+1) P_1 P_2 \dots$. It is an integer with which $P_m \leq 2^n$ is filled.

[0024] Next operation of the pseudorandom-numbers generator 2 constituted in this way is explained. If one clock pulse of a clock signal is inputted through the input terminal 180 the random number generator 101 The integer A (pseudorandom numbers) with which $0 \leq A < (P_1-1)(P_2-1) \dots (P_m-1)$ is filled synchronizing with the clock pulse is generated at random and divider 102_1 is supplied (random number generation step concerning this invention).

[0025] On the other hand divider 102_1 computes quotient $D_2=A/(P_1-1)$ when the pseudorandom numbers A are \ast (ed) for an integer (P_1-1) and the surplus $A \bmod (P_1-1)$ Output a quotient and a surplus and each divider 102_k ($k=2\text{---}m$) Compute quotient $D_{k+1}=D_k/(P_k-1)$ when quotient D_k which left-hand side divider 102_{k-1} outputs is \ast (ed) for an integer (P_k-1) and surplus $D_k \bmod (P_k-1)$ and a quotient and a surplus are outputted. A surplus is outputted to adding machine 103_k corresponding respectively (division step concerning this invention). Below it is written as expedient upper $D_1=A$ of explanation. And each adding machine 103_k from each remainder arithmetic machine 102_k to surplus $D_k \bmod (P_k-1)$, "1" inputted through the input terminal 192 is

added and result $B_k (= \{D_k \bmod (P_k - 1) + 1\})$ is outputted to corresponding multiplier 104_k (the 1st summing step concerning this invention). Multiplier 104_k multiplies by integer $a_k (P_1 P_2 \dots P_m / P_k)$ inputted through input terminal 193_k corresponding to this added result B_k . A result is outputted to the adding machine 105 (multiplication step concerning this invention).

[0026] Then the adding machine 105 adds all outputs of each multiplier 104_k outputs an added result to the remainder arithmetic machine 106 (the 2nd summing step concerning this invention) and the remainder arithmetic machine 106 integer $P_1 P_2$ into which an added result from the adding machine 105 is inputted through the input terminal 194 A surplus when it \times by P_m is computed and it outputs to the adding machine 107 as the integer X (remainder arithmetic step concerning this invention). [0027] And integer $Q P_1 P_2$ as which the adding machine 107 is inputted into the above-mentioned integer X from the remainder arithmetic machine 106 through the input terminal 195 P_m is added. An acquired integer (pseudorandom numbers) is outputted from the output terminal 196 as a candidate of a prime number used as a secret key (the 2nd arithmetic step concerning this invention). The above-mentioned integer X computed based on [an one number] is $0 < X < P_1 P_2 \dots$. Since it is an integer with which P_m is filled it is not necessarily the desired number of bits i.e. an integer of n bit. With however the adding machine 107. Condition $2^{n-1} \leq Q P_1 P_2 [\dots P_m] < P_m$ and $(Q+1) P_1 P_2 \dots$. It is the integer Q with which $P_m \leq 2^n$ is filled. Integer $Q P_1 P_2 \dots$ by which P_m was multiplied. An integer of n bit is acquired by adding to the integer X . As a result whenever a clock pulse is inputted into the random number generator 101 through the input terminal 180 a candidate of a prime number of n bit for considering it as a secret key in a public-key crypto system is outputted one after another through the output terminal 196. When a value of the above-mentioned m obtains pseudorandom numbers with higher probability that it is a prime number to choose in the range in which a value of Q exists as greatly as possible it is preferred.

[0028] Why the integer X can serve as a candidate of a prime number about how the above [one number] is drawn here is explained in detail. The above-mentioned integer B_k expressed with $B_k = \{D_k \bmod (P_k - 1) + 1\}$ fills $0 < B_k < P_k$ to given arbitrary nonnegative integer D_k . It is $B_k \neq 0$ if it is $0 < B_k < P_k \pmod{P_k}$. Therefore if it is $P_1 P_2 \dots$ a prime number in which P_m is different. A primary alliance congruence expression If a solution of $X = B_1 \pmod{P_1}, X = B_2 \pmod{P_2}, \dots, X = B_m \pmod{P_m}$ exists and the solution is set to X (the above-mentioned integer X) X can be divisible by neither P_1 nor P_2 nor nor P_m . That is small prime number $P_1 P_2 \dots$ probability that X is a prime number become higher than probability that an integer generated only at random [X / it will be said that it does not have P_m in a prime factor and] is a prime number.

[0029] And the solution X of the above-mentioned primary alliance congruence expression $X = a_1 (P_1 P_2 \dots P_m / P_1) B_1 + a_2 (P_1 P_2 \dots P_m / P_2) B_2 + \dots + a_m (P_1 P_2 \dots P_m / P_m) B_m \pmod{P_1 P_2 \dots P_m}$. Asking simply is known by P_m and the 1st calculating means 4 computes the integer X by this one formula i.e. a [number].

[0030] Thus according to this embodiment if a random number generator generates one integer at random according to a predetermined computing equation ([one number]) one candidate of an integer with high probability which is a prime number i.e. a prime number will certainly be generated based on the integer. Therefore compared with a method which generates many integers at random like before and sorts out a prime number a candidate of a prime number can be obtained extremely in a short time. In order to investigate whether it is a prime number conventionally division needed to be done but division is unnecessary therefore it can constitute a device from this embodiment by low cost without using a divider.

[0031] The adding machine 107 is QP_1P_2 from the remainder arithmetic machine 106 to the integer $X \dots$. A result adding $P_m A$ candidate (pseudorandom numbers) of a prime number which is n bit which the adding machine 107 outputs. It will not be distributed over $Mr. \{2^{n-1} \dots 2^n - 1\}$ top **** but will be distributed over $Mr. \{P_m - QP_1P_2 \dots P_m \dots P(Q+1) \dots P_2 \dots 1\}$ top ****. Therefore although he cannot call it ideal pseudorandom numbers statistically since a candidate of a prime number of this n bit uses a candidate of a generated prime number in order to obtain a secret key of public key encryption this embodiment is enough for him in such a case.

[0032] Next a 2nd embodiment is described. Drawing 2 is a functional block diagram showing a 2nd embodiment of a pseudorandom-numbers generator by this invention. Below with reference to this figure a 2nd embodiment of a pseudorandom-numbers generator by this invention is described and an embodiment of a pseudorandom-numbers generation method by corresponding this invention is described simultaneously. The same numerals are given to the same element as drawing 1 among drawing 2 and explanation about them is omitted here.

[0033] The random number generator 101 of drawing 1 is replaced by two or more random number generator 201_k and that this pseudorandom-numbers generator 6 differs from the pseudorandom-numbers generator 2 of drawing 1 is the point that each divider 102_k is deleted in the 1st calculating means 5 equivalent to the 1st calculating means 4. Namely in this pseudorandom-numbers generator 6 random number generator 201_k is provided corresponding to each adding machine 103_k . A clock signal is inputted into each random number generator 201_k through the input terminal 180 and an integer $(P_k - 1)$ is supplied through input terminal 290_k corresponding to each random number generator 201_k . and as for each random number generator 201_k each clock pulse of a clock signal is inputted -- alike -- $0 \leq A_k < (P_k - 1)$ -- pseudorandom-numbers A_k to fill is generated and is outputted to corresponding adding machine 103_k . And in this pseudorandom-numbers generator 6 each random number generator 201_k generating pseudorandom-numbers A_k equivalent to integer $D_k \bmod (P_k - 1)$ which the above-mentioned divider 102_k (drawing 1) outputs each part after adding machine 103_k operates like a case of the above-mentioned embodiment and generates an integer of n bit as a candidate of a prime number. Therefore although the same effect as a case of the above-mentioned

embodiment is acquired and the number of random number generators also increases this embodiment by this embodiment further since m dividers become unnecessary a candidate of a prime number is further generable at a high speed from the above-mentioned embodiment.

[0034] Next a 3rd embodiment is described. Drawing 3 is a functional block diagram showing a 3rd embodiment of a pseudorandom-numbers generator by this invention. Below with reference to this figure a 3rd embodiment of a pseudorandom-numbers generator by this invention is described and an embodiment of a pseudorandom-numbers generation method by corresponding this invention is described simultaneously. The same numerals are given to the same element as drawing 2 among drawing 3 and explanation about them is omitted here.

[0035] That this pseudorandom-numbers generator 8 differs from the pseudorandom-numbers generator 6 of drawing 2. Each multiplier 104_k of drawing 2 is replaced by ROM (read only memory) 301_k respectively. The remainder arithmetic machine 106 is the point currently replaced by adding machine 303_1 , 303_2 and ROM 302_1 and 302_2 . First an added result of each adding machine 103_k is inputted into an address terminal of each ROM 301_k and data which each ROM 301_k holds is supplied to the adding machine 105 from a data output terminal of each ROM 301_k . (y at y address of each ROM 301_k And nonnegative integer) A value of integer $a_k(P_1P_2 \dots P_m/P_k)$ y is written in as data therefore each ROM 301_k achieves the same function as each multiplier 104_k . Integer B_k is inputted into each ROM 301_k from each adding machine 103_k and this value is small. Therefore since ROM with the small maximum of an address of each ROM 301_k and a small storage capacity can be used such composition is easily realizable.

[0036] On the other hand a bit by the side of a low rank among two or more bits which constitute output data of the adding machine 105 to one input terminal of adding machine 303_1 . The remaining bits are supplied to an address terminal of ROM 302_1 respectively and output data of ROM 302_1 is supplied to an another side input terminal of adding machine 303_1 . Inside of two or more bits which constitute output data of adding machine 303_1 a bit by the side of a low rank is supplied to one input terminal of adding machine 303_2 the remaining bits are supplied to an address terminal of ROM 302_2 respectively and output data of ROM 302_2 is supplied to an another side input terminal of adding machine 303_2 .

[0037] At z address (z is a nonnegative integer) of each ROM 302_1 and 302_2 . A value of integer $2^z \pmod{P_1P_2 \dots P_m}$ is written in as data. As a result these adding machine 303_1 , 303_2 and ROM 302_1 and 302_2 achieve a function of the remainder arithmetic machine 106 and the integer X is outputted from adding machine 303_2 . the integer z inputted into each ROM 302_1 and 302_2 -- at most -- it is m and since a value of m is small ROM with a small storage capacity can be used and such composition can be realized easily.

[0038] According to this 3rd embodiment at still high speeds since the same effect as a

case of the pseudorandom-numbers generator 6 mentioned above is acquired and a multiplier and a remainder arithmetic machine are not used further a candidate of a prime number can be generated. Although a multiplier and a remainder arithmetic machine which constitute a 2nd embodiment were replaced with ROM or an adding machine in this 3rd embodiment of course it is also possible to replace a multiplier and a remainder arithmetic machine with ROM or an adding machine similarly in a 1st embodiment and to attain improvement in the speed of processing.

[0039]

[Effect of the Invention] As explained above the pseudorandom-numbers generation method of this invention is provided with the following.

For m a positive integer P_1, P_2, \dots, P_m as two or more prime numbers The random number generation step which generates the pseudorandom numbers A which fill $0 \leq A < (P_1 - 1)(P_2 - 1) \dots (P_m - 1)$ by a random number generation means based on given integer $(P_1 - 1)(P_2 - 1) \dots (P_m - 1)$.

The integer expressed with $D_1 = A$ by formula $D_k = D_{k-1} / (P_k - 1)$ to the integer k below or more $2m$ in D_k Two or more integers expressed by formula $[D_k \bmod (P_k - 1)] + 1$ to positive integer k below m in B_k And as two or more integers with which congruence expression $a_k(P_1 P_2 \dots P_m / P_k) \equiv 1 \pmod{P_k}$ is filled a_k Formula $a_1 \cdot (P_1 P_2 \dots P_m / P_1) B_1 + a_2(P_1 P_2 \dots P_m / P_2) B_2 + \dots + a_m(P_1 P_2 \dots P_m / P_m) B_m \pmod{P_1 P_2 \dots P_m}$ The 1st arithmetic step that computes the integer X expressed by P_m using a remainder arithmetic means an adding means and a multiplication means

They are a positive integer and Q about n Condition $2^{n-1} \leq Q P_1 P_2 \dots P_m$ and $(Q+1) P_1 P_2 \dots$ as an integer with which $P_m \leq 2^n$ is filled It is integer $Q P_1 P_2$ to said integer X by an adding means.... The 2nd arithmetic step that adds P_m generates an integer and is outputted

[0040] The pseudorandom-numbers generator of this invention is provided with the following.

For m a positive integer P_1, P_2, \dots, P_m as two or more prime numbers A random number generation means to generate the pseudorandom numbers A which fill $0 \leq A < (P_1 - 1)(P_2 - 1) \dots (P_m - 1)$ based on inputted integer $(P_1 - 1)(P_2 - 1) \dots (P_m - 1)$.

The integer expressed with $D_1 = A$ by formula $D_k = D_{k-1} / (P_k - 1)$ to the integer k below or more $2m$ in D_k Two or more integers expressed by formula $[D_k \bmod (P_k - 1)] + 1$ to positive integer k below m in B And as two or more integers with which congruence expression $a_k(P_1 P_2 \dots P_m / P_k) \equiv 1 \pmod{P_k}$ is filled a_k Formula $a_1 \cdot (P_1 P_2 \dots P_m / P_1) B_1 + a_2(P_1 P_2 \dots P_m / P_2) B_2 + \dots + a_m(P_1 P_2 \dots P_m / P_m) B_m \pmod{P_1 P_2 \dots P_m}$ The 1st calculating means including the remainder arithmetic means adding means and multiplication means which compute the integer X expressed by P_m

They are a positive integer and Q about n Condition $2^{n-1} \leq Q P_1 P_2 \dots P_m$ and $(Q+1) P_1 P_2 \dots$ as an integer with which $P_m \leq 2^n$ is filled It is integer $Q P_1 P_2$ to said integer X The 2nd calculating means that adds P_m generates an integer and is outputted

[0041] That is in this invention since the integer X with high probability which is a prime number is computed based on predetermined expression from the pseudorandom numbers A one candidate of a prime number is certainly generated to the one pseudorandom numbers A. Therefore compared with the method which generates many integers at random like before and sorts out a prime number the candidate of a prime number can be obtained extremely in a short time. In order to investigate whether it is a prime number conventionally division needed to be done but division is unnecessary therefore it can constitute a device from this invention by low cost without using a divider.

[0042] The pseudorandom-numbers generation method of this invention is provided with the following.

The positive integer below $mP_1P_2 \dots$ and P_m for a positive integer and k as two or more prime numbers [m] being based on two or more given integers $(P_1-1)(P_2-1) \dots$ and $(P_m-1) \rightarrow 0 \leq A_k \rightarrow (P_k-1) \rightarrow$ the random number generation step which generates two or more pseudorandom-numbers A_k to fill by two or more random number generation means respectively.

Two or more integers expressed by formula A_k+1 in B_k and a_k as two or more integers with which congruence expression $a_k(P_1P_2 \dots P_m/P_k) \equiv 1 \pmod{P_k}$ is filled Formula $a_1 \cdot (P_1P_2 \dots P_m/P_1) B_1 + a_2(P_1P_2 \dots P_m/P_2) B_2 + \dots + a_m(P_1P_2 \dots P_m/P_m) B_m \pmod{P_1P_2 \dots P_m}$.

The 1st arithmetic step that computes the integer X expressed by P_m using a remainder arithmetic means an adding means and a multiplication means

They are a positive integer and Q about n Condition $2^{n-1} \leq QP_1P_2 \dots P_m$ and $(Q+1)P_1P_2 \dots$ as an integer with which $P_m \leq 2^n$ is filled It is integer QP_1P_2 to said integer X by an adding means.... The 2nd arithmetic step that adds P_m generates an integer and is outputted

[0043] The pseudorandom-numbers generator of this invention is provided with the following.

The positive integer below $mP_1P_2 \dots$ and P_m for a positive integer and k as two or more prime numbers [m] being based on two or more integers (P_1-1) and (P_2-1) which were inputted and $(P_m-1) \rightarrow 0 \leq A_k \rightarrow (P_k-1) \rightarrow$ two or more random number generation means to generate two or more pseudorandom-numbers A_k to fill respectively.

Said two or more integers expressed by formula A_k+1 in B_k And as two or more integers with which congruence expression $a_k(P_1P_2 \dots P_m/P_k) \equiv 1 \pmod{P_k}$ is filled a_k Formula $a_1 \cdot (P_1P_2 \dots P_m/P_1) B_1 + a_2(P_1P_2 \dots P_m/P_2) B_2 + \dots + a_m(P_1P_2 \dots P_m/P_m) B_m \pmod{P_1P_2 \dots P_m}$. The 1st calculating means including the remainder arithmetic means adding means and multiplication means which compute the integer X expressed by P_m

They are a positive integer and Q about n Condition $2^{n-1} \leq QP_1P_2 \dots P_m$ and $(Q+1)$

$P_1 P_2 \dots$ as an integer with which $P_m \leq 2^n$ is filled. It is integer $Q P_1 P_2$ to said integer $X \dots$.
The 2nd calculating means that adds P_m generates an integer and is outputted

[0044] That is in this invention since the integer X with high probability which is a prime number is computed based on predetermined expression from two or more pseudorandom-numbers A_k , one candidate of a prime number is certainly generated to pseudorandom-numbers A_k constructed one. Therefore compared with the method which generates many integers at random like before and sorts out a prime number, the candidate of a prime number can be obtained extremely in a short time. In order to investigate whether it is a prime number conventionally, division needed to be done, but division is unnecessary, therefore it can constitute a device from this invention by low cost without using a divider.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is a functional block diagram showing the 1st embodiment of the pseudorandom-numbers generator by this invention.

[Drawing 2] It is a functional block diagram showing a 2nd embodiment of the pseudorandom-numbers generator by this invention.

[Drawing 3] It is a functional block diagram showing a 3rd embodiment of the pseudorandom-numbers generator by this invention.

[Drawing 4] It is a flow chart which shows how to generate the candidate of the conventional prime number.

[Description of Notations]

268 A pseudorandom-numbers generator 45 ---- The 1st calculating means 101 201

$1_{201} 2_{201} \dots$ A random number generator 105 and 107 103 $1_{103} 2_{103} \dots$ 302 $1_{302} 2_{302} \dots$

Adding machine 106 102 $1_{102} 2_{102} \dots$ Remainder arithmetic machine 104 $1_{104} 2_{104} \dots$

A multiplier 301 $1_{301} 2_{301} \dots$ 302 $1_{302} 2_{302} \dots$ ---- ROM (read only memory).
